REMARKS

In the Office Action, the Examiner rejected Claims 1-21, which were all of the then pending claims, under 35 U.S.C. 103 as being unpatentable over the prior art. In particular, Claims 1-16, 18 and 20 were rejected as being unpatentable over U.S. Patent 6,519,700 (Ram, et al.) in view of U.S. Patent 6,247,127 (Vandergeest) and further in view of U.S. Patent 6,138,119 (Hall). Claims 17, 19 and 21 were rejected as being unpatentable over Ram, et al. in view of Vandergeest and Hall and further in view of U.S. Patent 6,775,655 (Peinado).

Independent Claims 1, 6, 10, 14, 18 and 20 are being amended to better define the subject matters of these claims. Also, new Claim 22, which is dependent from Claim 6, is being added to describe a preferred feature of the invention, and Claim 21 is being cancelled to reduce the number of issues in this application.

For the reasons set forth below, Claims 1-10 and 22 patentably distinguish over the prior art and are allowable. The Examiner is thus asked to reconsider and to withdraw the rejection of Claims 1-20, and to allow these claims and new Claim 22.

The main differentiating point between this invention and the referenced prior art is that the prior art requires customization of the player application whereas this invention does not. The merit of this invention lies in enabling usage of standard uncustomized players to play back content protected by digital rights, i.e., the ability to use a player, the code of which is neither obfuscated nor placed in a tamper resistant environment, and still be able to utilize it to play back the content securely. More importantly, this invention does not require the player code to be changed in any way. It is not required to exchange a trust certificate, access/decrypt digital rights, or decrypt the protected content. The essential requirement from the player is to have a content handler extension mechanism, which is a capability found in many modern players. That mechanism is used in the present invention to provide a trusted content handler that handles the rights and protected content, and passes the decrypted content to the player to play. Execution control is passed between the player and content handler, and that necessitates verification of the entity (the player), which the trusted content handler is passing content and control to, to make sure that it is not a modified malicious version of the player.

In contrast to the main goal of this invention of using standard players, Ram teaches how to use a special secure trusted player, which implements all the functions to access and decrypt the protected content, and which is bundled with the content in an SPD. Ram also teaches an alternative embodiment using a trusted viewer/player, which is connected to the SPD via protocols and interfaces. Ram does not teach how to use a standard "untrusted" player. It also does not teach how to authenticate and verify the integrity of the player in this case.

Vandergeest describes a procedure for secure off-line communications. Generally, in this procedure, information is exchanged between two end users to enable them to go off line and to participate in secure communications.

Hall discloses rights management data structures. As an example, one data structure may comprise an abstract data representation of the format of the data. This representation may be used to create rights management data structures, allow others to read and understand such data structures, and to manipulate some or all of the data structures. Hall was cited in the Office Action for disclosing linking applications and/or programs at run time.

Peinado also teaches how to use a rendering application that is connected to a DRM system via an authentication protocol. Peinado does not teach how to perform authentication and verification of a standard "untrusted" player.

Both Ram and Peinado regard the player application as a single monolithic unit that is either trusted or implements specific authentication protocol/interface. None of the referenced prior art touches the issue of using an existing extension mechanism of a standard player to implement DRM functions. In this invention, the player application is divided into a core rendering application that is not to be modified in order to support protected content, and an extension mechanism (content handler) that a trusted version of which can be easily provided to supplement the player.

In response to the Examiner's comments in paragraph 2(a) of the Office Action, the verification system of this invention and Ram's rights enforcer are not similar components, as the Examiner's comments implies. The verification system's purpose is to validate the integrity of the player application. It does not handle the usage rights or the content. Ram's rights enforcer validates the user identify and handles the usage rights.

Also, as stated earlier, while the two flows (Ram's and the present invention) may look similar on the face, there is a critical difference, which is that Ram's rendering application is a special trusted application that is designed to interface to the rights enforcing component. It can be regarded as an extension of the rights enforcer, and in fact, in their preferred embodiment, the rendering application is part of the SPD. In the present invention, the player (rendering application) is DRM agnostic.

Also, whether the functional blocks (verification system, trusted content handler, and user interface control module) are implemented in hardware or software is irrelevant. While the Examiner rightfully notes that these functional blocks may be consolidated or separated, their independence from the player application is the point that is sought here and is not taught by the cited prior art.

With regard to the Examiner's rejection of Claim 4, in paragraph 3(b) of the Office Action, applicants respectfully note that the Examiner appears to confuse user authentication with player authentication. User authentication, as taught in Ram, is necessary to exercise the rights associated with the content. The player authentication mentioned in depende4nt Claim 4 is different. It is a part in the algorithm for verifying the integrity of the independent player application. It complements the role of the verification system.

With respect to the rejection of Claim 5, the function of the user interface control module is totally different and has nothing to do with Ram's SPD distribution scheme. This UI control module is effective at a later stage after the distribution of content (or SPD) is complete. It is necessary, in the case of an independent player, to make sure that the rights are not violated while the user is using the standard player application's interface.

With respect to the rejection of Claim 3, the function of the verifying launcher, which is used to verify the integrity of the player application, is different from Ram's enforcement of rights, or allowing usage of content in accordance with the associated rights. The Examiner refers to "verification of conditions associated with rights is performed using SPD" given in Ram, without specifying what conditions are meant in this context or how to verify these conditions.

Independent Claims 1, 6, 10, 14, 18 and 20 are being amended to emphasize differences between the claims and the prior art. For instance, Claims 1, 6 and 10 are being amended to describe the feature that the player applications have a core rendering application and an extension mechanism, and that the digital rights management system of this invention uses this extension mechanism of the player application to implement the functions of the digital rights management system without modifying the core rendering application.

Claims 14, 18 and 20 presently describe an authenticator used to verify that requests from player applications have been authorized. These claims are being amended to describe the feature that the player applications have a core rendering application and an extension mechanism, and that the above-mentioned authenticator uses this extension mechanism of the player application to implement the functions of the authenticator without modifying the core rendering application.

The above-discussed features of the invention are of utility because they enable a digital rights management system that effectively manages digital rights, and at the same time is very flexible and minimally intrusive, and does not put any conditions on the type of the contents that need to be delivered, or on the applications used to access those contents.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also fail to disclose this use of the certificate generator.

In view of the above-discussed differences between Claims 1, 6, 10, 14, 18 and 20 and the prior art, and because of the advantages associated with those differences, Claims 1, 6, 10, 14 and 18 patentably distinguish over the prior art and are allowable. Claims 2-5 are dependent from Claim 1 and are allowable therewith; and Claims 7-10 and 22 are dependent from, and are allowable with, Claim 6. Also, Claims 11-13 are dependent from Claim 10 and are allowable therewith; and Claims 15-17 are dependent from Claim 14 and are allowable therewith. Claim 19 is dependent from, and is allowable with, Claim 18.

For the reasons discussed above, the Examiner is respectfully requested to reconsider and to withdraw the rejection of Claims 1-20 under 35 U.S.C. 103, and to allow these Claims and new Claim 22. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S Sensny
John S. Sensny
Registration No. 28,757
Attorney for Applicants

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343
Customer No. 23389

JSS:jy